Owning all the data all the time: aspects of *Surveillance Capitalism*

Abstract

This report attempts to survey some elements surrounding the notion of *Surveillance Capitalism*, a term initially defined by Zuboff (2015) to describe how – by surreptitiously collecting user-data from everyday digital connections between apps, operating systems, devices and their capitalist masters – private human experience has been digitised and commoditised, and behaviour is modified. The paper is an effort to provide a broad literature review of some aspects related to this burgeoning field of research. This report does not seek solutions, it simply endeavours to offer a brief overview of several disparate concepts within this complex digital environment.

Introduction

As we enter the third decade of the 21st century, throughout the Global North, the data-detritus of our digital existence is a raw, natural resource for data-mining tech giants to create rampant wealth – as they quietly invent a highly successful new type of capitalism (Pettis, 2020; Sandberg, 2020). The relatively new hypothesis of *Surveillance Capitalism* can be described as the economic process of tracking, collecting, analysing, and commodifying personal user-data to modify human behaviour (Andrew & Baker, 2019; Naughton, 2019; Zuboff, 2016). Originally coined by Harvard Professor Shoshana Zuboff (2015), this predominantly furtive version of digital capitalism utilises data generated from everyday internet use – a user's individual digital footprint – and allows data-tracking oligopolies, mostly large big-data tech companies and media corporations to reap a profit from user behaviour (Kelley, 2020) – with a view to modify and commoditise that behaviour.

Surveillance Capitalism goes beyond the scope of simply targeted advertising, rather the practice is based on selling predictions of our futures to businesses who are willing to pay for it (Zuboff, 2019c). The Surveillance Capitalists hope to maximise profit by knowing exactly what people will do next – and this is fodder for profit. Notably in insurance, real estate, health, education, government – ostensibly every sector within the contemporary capitalist ecosystem (Zuboff, 2019a) – but at what cost? Does this relatively new economic reality, this secret process of data capitalism without real consent, undermine democratic and human rights?

Literature Review and concerns

Google/Alphabet, Facebook, Amazon, Apple and Microsoft – often known as the *big five* or "FAAMG" – leaders of the so-called *now economy* (Weinstein, 2020) – develop comprehensive data-profiles of users as they traverse increasingly essential platforms and devices throughout their virtual lives (Wood & Monahan, 2019). This often surreptitious and mostly misunderstood practice of mandatory data collection generously gifts an enormous amount of real-time personal information to a relatively small number of global enterprises (Robertson, 2020).

The *big five*, motivated by neoliberal market ideals, have been described as the "gatekeepers to all online social traffic and economic activities" (van Dijck, 2020). It is said that their combined services directly and fundamentally impact society, affect democracy and drive the global economy (Maas, 2020; Schia & Gjesvik, 2020). Indeed, during the pandemic recession of 2020, the tech conglomerates – including those producing hardware devices – accounted for around 40% of the S&P 500, with the greatest ever historical share of the U.S. stock market, surpassing even the dot-com boom heights of early 2000 (Amrith, 2020; Kshetri, 2020; Ziemba, 2020).

The apparently innocuous user-data is collected and analysed within the technology frameworks of *big data*, using widespread sophisticated algorithms, including *artificial intelligence* and *machine learning* to create monetary streams – signalling the logic of *data capitalism* (Robinson, 2020). Data capitalism, in which the commoditisation of data results in a lopsided redistribution of economic power, slants toward those with exclusive access to evaluate that information (Jacquinet, 2019; West, 2019) – i.e. the big tech giants.

As an example, Google's suite of products, including its market-dominant and highly ubiquitous search engine, its Google Assistant and Google Home products; Amazon's Alexa; and Apple's Siri are all potential extraction conduits for personal data to be commoditised in myriad ways (Chaudhary, 2020). Facebook, Instagram, WhatsApp to list a few are also prime fodder for surveillance capitalism corporations (Lyon, 2019).

Whilst the "use of personal data in advertising, strategic marketing, and client management is nothing new" (Cinnamon, 2017), Surveillance Capitalism's goal is to "predict and modify human behaviour as a means to produce revenue and market control" (Zuboff, 2015). This

goal becomes easier as more data is created and collected. And data growth is indeed abundant as we consume more devices and consume/create even more data. Today, "the number of smartphone-users worldwide surpasses three billion and is forecast to grow by another several hundred million over the next few years" (Statistica, 2020b). The overall amount of data collected doubles every two years, with an estimated 44 zettabytes – one zettabyte equals one million petabytes or one billion terabytes (Yu & Song, 2020) – by the end of 2020 (Martha, 2020). Recent analysis shows that 3.96 billion people used social media in July 2020 – accounting for roughly 51 percent of the global population; more than 376 million new users since July 2019, which equates to approximately 12 new users every second (DataReportal, 2020).

From this massive and increasing usage comes increasingly massive amounts of user-data. Bigger data-sets allow deeper insights from the data exhaust created from the movement across virtual connections – indeed the resource of residual user-data has become a "data gold mine" for business optimisation, embracing the move toward a digital capitalist revolution through the ongoing use of big data and its cousin, big data analytics (Ochs & Riemann, 2018).

There are many documented benefits of commercial and proprietary apps which, by tracking digital exhaust, can provide useful insights into aspects of life. Data about behaviour can assist with: health issues, enabling users to improve health based on otherwise unknown data – sleep patterns and mental health for example – yet issues of digital privacy and breaches of confidentiality remain (Haidt & Allen, 2020; Lustgarten et al., 2020; Milne-Ives et al., 2020); collecting contact tracing information in a pandemic, albeit often without governance (Leith & Farrell, 2020; Rowe, 2020); in remote work and work-from-home situations, as mobile enterprise applications improve the organisation of people and data, and add value for stakeholders, but may also destabilise once hard-fought-for equitable workplaces (Leonardi, 2020; Molin, 2020).

According to Zuboff (2019a, p. The Definition), Surveillance Capitalism is: "a rogue mutation of capitalism marked by concentrations of wealth, knowledge and power unprecedented in human history." The furtive way big tech companies, indeed, any company, can mine user-data is often considered ethically dubious: *click-wrap*, *browse-wrap*, *I-agree-button* consent

and other ambiguous click-through legal agreements where contract terms are not immediately conveyed to the consumer (Casey et al., 2020; Mozingo, 2020) are widely used. Surveillance Capitalists will claim legal ownership over, accumulate and analyse users' personal human-experience as a free source of raw capitalist material; raising the "rich predictive signals" (as Zuboff calls it) of human behaviour and turn that into useful behavioural information for their purposes – often in a highly opaque manner. This method of capitalism has been described as a manifest shift from 'mass production' in favour of 'mass predictive personalisation' (Fia, 2020; Yeung, 2018).

If consumers of platform services care to read the terms of agreements and privacy policies of big tech corporations, they may be concerned (Meier et al., 2020). Facebook's for example will advise users that all data, as well as connections with other users, or third-party users will be gathered up, shared and used for whatever purpose the company desires; users of Google's Search and Gmail must automatically accept that their "emails and searches are reviewed for future customizations" and further, "will send the user's browsing information to Google and its partners" (Vianna & Meneghetti, 2020).

With the ongoing, ever-expanding acceptance of online devices and apps, users of mobile phones, desktops, laptops, tablets, phablets and a plethora of smart devices, generate a vast and escalating volume of personal data as they negotiate their way through the necessary virtual networks of daily life. According to Statistica (2020a), almost 4.57 billion people were active internet users as of July 2020, comprising 59 percent of the global population. Add to this the Internet of Things (IoT) which incorporates billions of connected devices, sharing data between each other – with minimal human intervention – yet leaving digital traces of packet traffic with every connection. Note too, that IoT is one of the fastest developing fields in the history of computing, with an estimated 50 billion devices expected by decade's end (Al-Garadi et al., 2020).

Increasingly our lives are wholly dependent on internet connectivity. IoT has enabled the world around us to be linked ubiquitously to people and machines. And whilst the potential security vulnerabilities of a smart, ultra-connected environment are often noisily posited as a threat (Alladi et al., 2020; Yu et al., 2020), the more recent concept of Surveillance Capitalism has so far been overlooked.

The primary purpose of IoT technology is to streamline processes across various systems, to ensure greater efficiency and improve quality of life (Nižetić et al., 2020). From smart speakers, door-bells, watches, cameras, cars, fridges, TVs, toys, thermostats, lighting, medical devices etc, IoT is edging into the regular lives of people across the planet (Langley et al., 2020). Further, the Internet of *Everything* (IoE) develops IoT with digital relationships between data, people and processes – as the strings and code of real-time data flow between smart systems. Data security, as traffic moves from the pervasive and inexorably expansive IoE ecosystems and into the cloud sphere, is a major factor (Karthiban & Raj, 2019; Nezami & Zamanifar, 2019).

Nevertheless, the accumulated digital data, housed on integrated "cloud-computing" platforms can be collected, analysed and used for further purposes such as digital marketing opportunities for businesses – to enable competitive advantages, and can have significant impact on business profit (Saura, 2020; Wedel & Kannan, 2016). Data scraped from personal experience is entered into a supply chain for use in what Zuboff describes the "new factories," where Artificial Intelligence creates computational products which "predict our behaviour" (Zuboff, 2019b).

Whilst these "prediction products" are indeed *about us* - they are *not for us*; they are not products designed to enhance our own lives. Rather, these surveillance products are computations that endeavour to predict precisely "what individuals and groups will do now, and into the future;" they are sold to business customers who want competitive advantages on future behaviour (Zuboff, 2019c). And, rather than the internet being a mere platform of convenience, in almost every aspect of contemporary survival – in order to live an effective life – users are forced to parade through the supply chains of Surveillance Capitalists.

Surveillance Capitalism is not dissimilar to the concept of *platform capitalism.* Big tech platforms like Amazon Web Services, which maintains around 32 percent of the cloud infrastructure services market (Stastica, 2020), are focused on building (and owning) the platform systems needed to collect, analyse, and deploy data for other companies to use – the collection of immense volumes of data is key to their business model and these platforms provide the necessary systems to aggregate and analyse huge amount of big data (Srnicek, 2017, p. 89). This platform capitalism – a corporate model successfully demonstrated by

Google, Facebook, Apple, Amazon and Uber et-al – uses software-as-a- service to disseminate user-data for profit (Dyer-Witheford, 2020).

In platform capitalism every user interaction is a basis for "profit extraction" – trading products/services or selling user-data on to third parties. Digital platform development enables platform capitalists to collect and commoditise data, and deliver bespoke messaging to users as they cruise the surface of the world wide web (Balayan & Tomin, 2020), and as such, the concept merges well with Zuboff's Surveillance Capitalism.

As users increasingly leave their digital footprints (consciously or not) across the various pages and portals of the world wide web, this shadow behaviour data from mobile/smart phone usage, social media interactions, credit card usage, search history, swipe cards actions, smart travel cards on transport systems, smart-wear sensors etc – known as *data exhaust*, *digital exhaust* or *digital breadcrumbs* – were once considered waste material. Now, this highly valuable user-data user is described as a consumer *digital portrait* (Krasnov et al., 2019). Digital exhaust from browsing, shopping, socialising and the increasingly essential daily use of internet services (MyGov, Centrelink are an example) has intensified researchers and marketers to explore the value of the digital footprint (Arya et al., 2019; Huberty, 2015).

Indeed, at the genesis of the internet, this exhaust – otherwise a user-behaviour data by-product – was ignored and considered as waste, but in 2001 the then fledgling dot com company Google, realised these data streams were indeed useful "rich predictive signals" – the behavioural metadata which Zuboff has referred to as *behavioural surplus* has become a profitable tool for the Surveillance Capitalists (Azar, 2020; Ball, 2019; Mills, 2020).

The utilisation of cloud computing services, such as machine learning, artificial intelligence, data mining, data sharing, data processing and other data analysis helps reveal insights about user behaviour, enabling organisations and businesses to make more informed decisions to increase income streams (Microsoft, 2020; Wang et al., 2020).

This sheer volume of accumulated user-data – that is, data which cannot be presented, processed, or analysed using traditional technologies – is known as Big Data (Lee, 2017). The rise of Big Data is seen as a radical step up from traditional data analysis and possesses three main traits: volume, variety, and velocity (Ghasemaghaei & Calic, 2020). Volume implies the quantity of data, which are created and stored; variety relates to the different types of

gathered data, and velocity represents the speed of data creation, streaming and aggregation (Gerhardt et al., 2012; Kaisler et al., 2013; Sagiroglu & Sinanc, 2013)

Big Data, as Hashem et al. (2015) notes, has three key attributes: the data is abundant; the data is impossible to organise with normal database systems; and the data streams are generated, captured, and analysed quickly. Big Data analytics refers to the methods used to analyse, process and expose otherwise obscure underlying patterns, interesting relations and other insights (Iqbal et al., 2020). Surveillance Capitalists now utilise big data analytics to create new profit streams (Marr, 2017).

In 2020, it is estimated there are over 1.5 billion websites (Forum, 2020). Digitalisation encroaches every aspect of life today – it is a virtual requirement of the 2020 human experience (at least for digital residents of the Global North) to always be connected to a network (Costabile et al., 2020). Access to cheap tablets, smartphones and an increasing array of smart-wear enables network access to almost anybody, anytime, anywhere (Gaines, 2019). Within a relatively short space of time we cannot escape the digital *hyperconnectivity* of life – where everybody is connected to everybody, everywhere, always. Over the last decade we have become addicted (arguably by design), checking smartphones over 150 times a day (Neyman, 2017) to an rapidly increasing amount of digitality to endless digital content, everywhere and all the time (Brubaker, 2020; Pillay, 2020).

Thwaites (2020) outlines concerns that big tech corporations are rapidly increasing their market control over hyperconnectivity – that the human condition is at stake. Globalisation and technology are:

> "promoting a rootlessness for human societies. Deregulation, outsourcing and relocation in the world of work, international business open 24/7 globally, and the powerful technology giants often replacing or overriding the foreign policies of nations and the autonomy of city states, all generate an instability in social life."

And hyperconnectivity is not just about people, it includes IoT and is always listening, continuously capturing troves of personal information so vast and voluminous the "data deluge" must be stored in so-called *data lakes* (Beheshti et al., 2020; Laurent et al., 2020).

The data interactions between machines, apps, operating systems and humanity's insatiable desire to document their lives online (via the platforms of Facebook, Instagram, YouTube TikTok etc) mean that a "large portion of everyone's daily activities and communications are part of a semi-permanent record" (Fredette et al., 2012). Once captured this data no longer belongs to the data subject (Hummel et al., 2020).

The implications of big data surveillance are vast. It was not until 2013 when Edward Snowden, a security contractor for the US Government revealed how an expansive global surveillance infrastructure – used by the "Five Eyes" countries (and other nations, including Singapore, Germany, South Korea and others) of the secret service global cabal – monitors and analyses the real time data of millions of citizens (Couch, 2019; Heikkilä, 2020; Lyon, 2015). The big data tech companies implicated in Snowden's surveillance revelations include Apple, Facebook, Google, Microsoft, Microsoft (i.e. the *big five*) – as well as other big data practitioners use, in Fuch's words:

> "algorithms that use instrumental logic for calculating human needs… automate human activities and decision-making in order to meet those needs. The problem is that algorithms and machines do not have ethics and morals." (Fuchs, 2019, p. 58)

The same could be said of the Surveillance Capitalists. At its most basic, capitalism takes things from outside a market and configures fresh ways to bring them into the marketplace to create new products and services to be sold and purchased. In the 21st century many natural resources are becoming increasingly depleted – and ironically incorporated and consumed into digital technology – and new sources of revenue are required for capital growth and evolution and a mutation of capitalist thinking is necessary (Fatehi & Taasoobshirazi, 2020; Kirsch, 2020). Hence, into and beyond the 2020s, capitalism demands fresh sources of margins, new things to commodify. Perhaps all that is left within the "systematic coercion of digital participation" for the successful capitalist in the ballooning digital surveillance economy are the raw material resources of human behavioural data (Barassi, 2019; Clarke, 2019).

When 98 percent of information is now digitised there is, as Zuboff (2019b) points out, a "foreclosure of alternatives," and whilst we may be well aware of the questionable

mechanisms of Surveillance Capitalism, users still have little choice but to be slaves to corporate giants. We are literally dependent on them. For example, access to school systems for education, especially in light of COVID-19 and recent lock-downs; access to personal health information; making plans with others, and organising events – the simple act of talking and messaging on a mobile phone creates data for the Surveillance Capitalists (Laidler, 2019). All employ the platforms and propriety products of big data centres such as Amazon, Google docs Microsoft etc. There is little escape.

Anecdotally, to highlight a point, the research for this very project resulted in constant multiple trackers being blocked at almost every new internet page of research, every PDF opened in a new browser created a "Allow Cookies" pop-up box. As key word searches for related papers via Google Scholar, browser data – such as IP address, site interaction data including time spent on a page, device and operating system data and versions, activity across various sites – apparently for insight on user interest, shopping habits and more is quietly collected (CookiePro, 2020). Pop-up cookie notices appear at almost every interaction. It has become part of the necessary journey of the internet and perhaps the gold mine of data payoff must be worth it – at least for the Surveillance Capitalists.

Cookies monitor user behaviour, enabling the cookie developers to identify sources of traffic, track clicks on a page – and by deploying web-analytics tools such as Google Analytics (Ranade, 2020; Semerádová & Weinlich, 2020), are used to examine user behaviour, and transform the collected information into a malleable resource for the data capitalist. With this information, a site can adapt or alter content, and present information accordingly (such as a price-adjustment for frequent visitors; different content dependent on user location) and may target advertising in a more tailored manner (Bornschein et al., 2020) – all with an overarching goal to achieve better profit outcomes and modify the user experience. The data crumbs of internet cookies are indeed currency.

Conclusion

The scope of this article was to briefly examine some of the concepts amid Surveillance Capitalism to help understand where the digital, capitalist surveillance economy may be heading. However, the sheer depth for the subject is far too complex for a few thousand words. Indeed, Professor Zuboff, in their seminal, ground-breaking tome, required over 700

pages, countless academic papers, newspaper and magazine articles, plus online interviews and discussions, but at least according to Lyon (2020), barely scratches the surface.

In summary, user-data is collected, stored and analysed to reside on a server somewhere, alongside all the other user behaviour information, in a data-centre lake in an undisclosed place, without any clear knowledge of what happens to that data. In the 21st century, the bits of information we unwittingly leave behind are the nuts and bolts of an emergent measureless market system – and as we traverse the digital malls and highways in our daily hyperconnected reality, the faceless behemoths of Surveillance Capitalism strive to "transform online behavioural information into data assets, and to attach these assets to advertising product" (Mellet & Beauvisage, 2020) – all to make us behave accordingly.

References

Alladi, T., Chamola, V., Sikdar, B., & Choo, K. R. (2020). Consumer IoT: Security Vulnerability Case Studies and Solutions. *IEEE Consumer Electronics Magazine*, *9*(2), 17-25.

Amrith, R. (2020, 16 October 2020). Tech's Influence Over Markets Eclipses Dot-Com Bubble Peak *The Wall Street Journal*. https://www.wsj.com/articles/techs-influence-over-markets-eclipses-dot-com-bubble-peak-11602894413

Andrew, J., & Baker, M. (2019). The General Data Protection Regulation in the Age of Surveillance Capitalism. *Journal of Business Ethics*. https://doi.org/10.1007/s10551-019-04239-z

Arya, V., Sethi, D., & Paul, J. (2019). Does digital footprint act as a digital asset? – Enhancing brand experience through remarketing. *International Journal of Information Management*, *49*, 142-156. https://doi.org/https://doi.org/10.1016/j.ijinfomgt.2019.03.013

Azar, M. (2020). POV-data-doubles, the dividual, and the drive to visibility. In *Big Data—A New Medium?* (pp. 177-190). Routledge.

Balayan, A. A., & Tomin, L. V. (2020, 8-8 April 2020). The Transformation of the Advertising Industry in the Age of "Platform Capitalism". 2020 IEEE Communication Strategies in Digital Society Seminar (ComSDS),

Ball, K. (2019). Review of Zuboff's The Age of Surveillance Capitalism. *Surveillance & Society*, *17*(1/2), 252-256.

Barassi, V. (2019). Datafied Citizens in the Age of Coerced Digital Participation. *Sociological Research Online*, *24*(3), 414-429. https://doi.org/10.1177/1360780419857734

Beheshti, A., Benatallah, B., Sheng, Q. Z., & Schiliro, F. (2020). Intelligent Knowledge Lakes: The Age of Artificial Intelligence and Big Data. In L. H. U, J. Yang, Y. Cai, K. Karlapalem, A. Liu, & X. Huang, *Web Information Systems Engineering* Singapore.

Bornschein, R., Schmidt, L., & Maier, E. (2020). The Effect of Consumers' Perceived Power and Risk in Digital Information Privacy: The Example of Cookie Notices. *Journal of*

Public Policy & Marketing, *39*(2), 135-154. https://doi.org/10.1177/0743915620902143

Brubaker, R. (2020). Digital hyperconnectivity and the self. *Theory and Society*, 1-31. https://link.springer.com/article/10.1007/s11186-020-09405-1

Casey, F., Nathan, B., & Brian, C. K. (2020). No Robots, Spiders, or Scrapers: Legal and Ethical Regulation of Data Collection Methods in Social Media Terms of Service. *Proceedings of the International AAAI Conference on Web and Social Media*, *14*(1). https://www.aaai.org/ojs/index.php/ICWSM/article/view/7290

Chaudhary, Z. R. (2020). The Politics of Exposure: Truth After Post-Facts. *ELH*, *87*(2), 301-324.

Cinnamon, J. (2017). Social injustice in surveillance capitalism. *Surveillance & Society*, *15*(5), 609-625.

Clarke, R. (2019). Risks inherent in the digital surveillance economy: A research agenda. *Journal of Information Technology*, *34*(1), 59-80. https://doi.org/10.1177/0268396218815559

CookiePro. (2020). *Website Tracking: Why and How Do Websites Track You?* Retrieved 16 October 2020 from https://www.cookiepro.com/blog/website-tracking/

Costabile, I., Kallegias, A., Robins, J. C., & West, T. N. (2020). The Corona Decade: The Transition to the Age of Hyper-Connectivity and the Fourth Industrial Revolution. *Transformation*.

Couch, B. (2019). Five Eyes: Unblinking, Unmoving, and Out of Control. *North Carolina Journal of International Law*, *45*(4), 25.

DataReportal. (2020). *Global Social Media Overview July 2020 DataReportal*. Retrieved 19 October 2020 from https://datareportal.com/reports/more-than-half-the-world-now-uses-social-media

Dyer-Witheford, N. (2020). Left Populism and Platform Capitalism. *tripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society*, *18*(1), 116-131.

Fatehi, K., & Taasoobshirazi, G. (2020). Contemplating the future: Mutating capitalism. *Thunderbird International Business Review*, *62*(2), 161-169. https://doi.org/doi:10.1002/tie.22113

Fia, T. (2020). An Alternative to Data Ownership: Managing Access to Non-Personal Data through the Commons. *Global Jurist*(0), 20200034. https://doi.org/https://doi.org/10.1515/gj-2020-0034

Forum, W. E. (2020). This is how many websites exist globally. https://www.weforum.org/agenda/2019/09/chart-of-the-day-how-many-websites-are-there/

Fredette, J., Marom, R., Steiner, K., & Witters, L. (2012). The promise and peril of hyperconnectivity for organizations and societies. *The global information technology report*, *2012*, 113-119.

Fuchs, C. (2019). Karl Marx in the Age of Big Data Capitalism. In D. Chandler & C. Fuchs (Eds.), *Digital Objects, Digital Subjects: Interdisciplinary Perspectives on Capitalism, Labour and Politics in the Age of Big Data* (pp. 53-71). University of Westminster Pres.

Gaines, B. R. (2019). From facilitating interactivity to managing hyperconnectivity: 50 years of human–computer studies. *International Journal of Human-Computer Studies*, *131*, 4-22. https://doi.org/https://doi.org/10.1016/j.ijhcs.2019.05.007

Gerhardt, B., Griffin, K., & Klemann, R. (2012). Unlocking value in the fragmented world of big data analytics. *Cisco Internet Business Solutions Group*, *7*.

Ghasemaghaei, M., & Calic, G. (2020). Assessing the impact of big data on firm innovation performance: Big data is not always better data. *Journal of Business Research*, *108*, 147-162. https://doi.org/https://doi.org/10.1016/j.jbusres.2019.09.062

Haidt, J., & Allen, N. (2020). Scrutinizing the effects of digital technology on mental health. *Nature*, *578*, 226. https://doi.org/10.1038/d41586-020-00296-x

Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A., & Ullah Khan, S. (2015). The rise of "big data" on cloud computing: Review and open research issues. *Information Systems*, *47*, 98-115. https://doi.org/https://doi.org/10.1016/j.is.2014.07.006

Heikkilä, H. (2020). Beyond Moral Coupling: Analysing Politics of Privacy in the Era of Surveillance. *Media and Communication*, *8*(2), 248-257.

Huberty, M. (2015). Awaiting the second big data revolution: from digital noise to value creation. *Journal of Industry, Competition and Trade*, *15*(1), 35-47.

Hummel, P., Braun, M., & Dabrock, P. (2020). Own Data? Ethical Reflections on Data Ownership. *Philosophy & Technology*. https://doi.org/10.1007/s13347-020-00404-9

Iqbal, R., Doctor, F., More, B., Mahmud, S., & Yousuf, U. (2020). Big data analytics: Computational intelligence techniques and application areas. *Technological Forecasting and Social Change*, *153*, 119253. https://doi.org/https://doi.org/10.1016/j.techfore.2018.03.024

Jacquinet, M. (2019). Artificial intelligence, big data, platform capitalism and public policy: an evolutionary perspective. *Going Digital*, 1-9.

Kaisler, S., Armour, F., Espinosa, J. A., & Money, W. (2013, 7-10 Jan. 2013). Big Data: Issues and Challenges Moving Forward. 2013 46th Hawaii International Conference on System Sciences,

Karthiban, M. K., & Raj, J. S. (2019). Big data analytics for developing secure internet of everything. *Journal of ISMAC*, *1*(02), 129-136.

Kelley, J. F. (2020). *Capitalism & Democracy in the Digital Age: Examining How the USA & Germany Enable & Disempower Surveillance Capitalism & Google* Leiden University]. Netherlands.

Kirsch, S. (2020). Running out? Rethinking resource depletion. *The Extractive Industries and Society*, *7*(3), 838-840. https://doi.org/https://doi.org/10.1016/j.exis.2020.06.002

Krasnov, S. V., Krasnov, A. S., & Bozhuk, S. S. (2019, 10-11 Oct. 2019). Transformation of Consumer's Digital Shadow in a Smart City. 2019 II International Conference on High Technology for Sustainable Development (HiTech),

Kshetri, N. (2020). COVID-19 Meets Big Tech. *Computer*, *53*(8), 10-13. https://www.computer.org/csdl/api/v1/periodical/mags/co/2020/08/09153302/1lSWbS25GdW/download-article/pdf

Laidler, J. (2019). *High tech is watching you*. The Harvard Gazette. https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy/

Langley, D. J., van Doorn, J., Ng, I. C. L., Stieglitz, S., Lazovik, A., & Boonstra, A. (2020). The Internet of Everything: Smart things and their impact on business models. *Journal of Business Research*. https://doi.org/https://doi.org/10.1016/j.jbusres.2019.12.035

Laurent, A., Laurent, D., & Madera, C. (2020). *Data Lakes*. John Wiley & Sons.

Lee, I. (2017). Big data: Dimensions, evolution, impacts, and challenges. *Business Horizons*, *60*(3), 293-303. https://doi.org/https://doi.org/10.1016/j.bushor.2017.01.004

Leith, D. J., & Farrell, S. (2020). Contact tracing app privacy: What data is shared by Europe's GAEN contact tracing apps. *Testing Apps for COVID-19 Tracing (TACT)*.

Leonardi, P. M. (2020). COVID-19 and the New Technologies of Organizing: Digital Exhaust, Digital Footprints, and Artificial Intelligence in the Wake of Remote Work. *Journal of Management Studies*, *n/a*(n/a). https://doi.org/10.1111/joms.12648

Lustgarten, S. D., Garrison, Y. L., Sinnard, M. T., & Flynn, A. W. P. (2020). Digital privacy in mental healthcare: current issues and recommendations for technology use. *Current Opinion in Psychology*, *36*, 25-31. https://doi.org/https://doi.org/10.1016/j.copsyc.2020.03.012

Lyon, D. (2015). *Surveillance after snowden*. John Wiley & Sons.

Lyon, D. (2019). Surveillance capitalism, surveillance culture and data politics. *Data Politics: Worlds, Subjects, Rights. Abingdon: Routledge*, 64-77.

Lyon, D. (2020). *The coronavirus pandemic highlights the need for a surveillance debate beyond 'privacy'*. The Conversation. Retrieved 23 October 2020 from https://theconversation.com/the-coronavirus-pandemic-highlights-the-need-for-a-surveillance-debate-beyond-privacy-137060

Maas, J. J. C. (2020). *The Power of Tech Companies : towards a non-dominating technology sector* [Masters thesis, University of Twente]. Netherlands. http://essay.utwente.nl/83612/

Marr, B. (2017). *Data strategy: How to profit from a world of big data, analytics and the internet of things*. Kogan Page Publishers.

Martha, D. (2020). Consumer Privacy Regulations: Considerations in the Age of Globalization and Big Data. In C. Gianluca, T. Abdellah, & M. Gabriel-Miro (Eds.), *Social, Legal, and Ethical Implications of IoT, Cloud, and Edge Computing Technologies* (pp. 222-238). IGI Global. https://doi.org/10.4018/978-1-7998-3817-3.ch010

Meier, Y., Schäwel, J., & Krämer, N. C. (2020). The Shorter the Better? Effects of Privacy Policy Length on Online Privacy Decision-Making [online privacy; privacy calculus; privacy policy; self-disclosure; social networking site]. *2020*, *8*(2), 11. https://doi.org/10.17645/mac.v8i2.2846

Mellet, K., & Beauvisage, T. (2020). Cookie monsters. Anatomy of a digital market infrastructure. *Consumption Markets & Culture*, *23*(2), 110-129. https://doi.org/10.1080/10253866.2019.1661246

Microsoft. (2020). *What is cloud computing?* https://azure.microsoft.com/en-au/overview/what-is-cloud-computing/

Mills, S. (2020). # DeleteFacebook: From Popular Protest to a New Model of Platform Capitalism? *Available at SSRN: https://ssrn.com/abstract=3541727 or http://dx.doi.org/10.2139/ssrn.3541727*.

Milne-Ives, M., van Velthoven, M. H., & Meinert, E. (2020). Mobile apps for real-world evidence in health care. *Journal of the American Medical Informatics Association*, *27*(6), 976-980. https://doi.org/10.1093/jamia/ocaa036

Molin, D. (2020). *Let them use apps : The integration and adoption of mobile enterprise applications* [Student thesis, DiVA. http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-282413

Mozingo, T. (2020). Revisiting the Enforceability of Online Contracts: The Need for Unambiguous Assent to Inconspicuous Terms. *Seattle University Law Review*, *43*(3).

Naughton, J. (2019). *'The goal is to automate us': welcome to the age of surveillance capitalism*. The Observer. https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook

Neyman, C. J. (2017). A survey of addictive software design. *California Polytechnic State University*.

Nezami, Z., & Zamanifar, K. (2019). Internet of Things/Internet of Everything: Structure and Ingredients. *IEEE Potentials*, *38*(2), 12-17. https://doi.org/10.1109/MPOT.2018.2855439

Nižetić, S., Šolić, P., López-de-Ipiña González-de-Artaza, D., & Patrono, L. (2020). Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. *Journal of Cleaner Production*, *274*, 122877. https://doi.org/https://doi.org/10.1016/j.jclepro.2020.122877

Ochs, T., & Riemann, U. (2018). Smart Manufacturing in the Internet of Things Era. In N. Dey, A. E. Hassanien, C. Bhatt, A. S. Ashour, & S. C. Satapathy (Eds.), *Internet of Things and Big Data Analytics Toward Next-Generation Intelligence* (pp. 199-217). Springer International Publishing. https://doi.org/10.1007/978-3-319-60435-0_8

Pettis, B. (2020). The costs of connection: how data is colonizing human life and appropriating it for capitalism. *Critical Studies in Media Communication*, *37*(2), 204-206. https://doi.org/10.1080/15295036.2020.1718835

Pillay, R. (2020). Digital Health Trends. In S. Wulfovich & A. Meyers (Eds.), *Digital Health Entrepreneurship* (pp. 207-213). Springer International Publishing. https://doi.org/10.1007/978-3-030-12719-0_15

Ranade, N. (2020). *The Real-Time Audience: Data Analytics and Audience Measurements* Proceedings of the 38th ACM International Conference on Design of Communication, Denton, TX, USA. https://doi.org/10.1145/3380851.3418613

Robertson, V. H. (2020). Excessive data collection: Privacy considerations and abuse of dominance in the era of big data. *Common Market Law Review*, *57*(1), 161-190.

Robinson, W. I. (2020). Global capitalism post-pandemic. *Race & Class*, *62*(2), 3-13. https://doi.org/10.1177/0306396820951999

Rowe, F. (2020). Contact tracing apps and values dilemmas: A privacy paradox in a neo-liberal world. *International Journal of Information Management*, *55*, 102178. https://doi.org/https://doi.org/10.1016/j.ijinfomgt.2020.102178

Sagiroglu, S., & Sinanc, D. (2013, 20-24 May 2013). Big data: A review. 2013 International Conference on Collaboration Technologies and Systems (CTS),

Sandberg, R. (2020). *Surveillance capitalism in the context of futurology: An inquiry to the implications of surveillance capitalism on the future of humanity* [Master's Thesis, University of Helsinki, Finland]. http://hdl.handle.net/10138/316996

Saura, J. R. (2020). Using Data Sciences in Digital Marketing: Framework, methods, and performance metrics. *Journal of Innovation & Knowledge*. https://doi.org/https://doi.org/10.1016/j.jik.2020.08.001

Schia, N. N., & Gjesvik, L. (2020). Hacking democracy: managing influence campaigns and disinformation in the digital age. *Journal of Cyber Policy*, 1-16. https://doi.org/10.1080/23738871.2020.1820060

Semerádová, T., & Weinlich, P. (2020). Using Google Analytics to Examine the Website Traffic. In *Website Quality and Shopping Behavior: Quantitative and Qualitative Evidence* (pp. 91-112). Springer International Publishing. https://doi.org/10.1007/978-3-030-44440-2_5

Srnicek, N. (2017). *Platform capitalism*. John Wiley & Sons.

Stastica. (2020). *Global market share of cloud infrastructure services from 2017 to 2020, by vendor* Retrieved 21 October 2020 from

https://www.statista.com/statistics/477277/cloud-infrastructure-services-market-share/
Statistica. (2020a). *Global digital population as of July 2020*. Retrieved 19 October 2020 from https://www.statista.com/statistics/617136/digital-population-worldwide/
Statistica. (2020b). *Number of smartphone users worldwide from 2016 to 2021 (in billions)* Retrieved 21 Oct 2020 from https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/
Thwaites, T. (2020). Technologizing the human condition: hyperconnectivity and control. *Educational Philosophy and Theory*, 1-10. https://doi.org/10.1080/00131857.2020.1806052
van Dijck, J. (2020). Governing digital societies: Private platforms, public values. *Computer Law & Security Review*, *36*, 105377. https://doi.org/https://doi.org/10.1016/j.clsr.2019.105377
Vianna, F. R. P. M., & Meneghetti, F. K. (2020). Is it crowdsourcing or crowdsensing? An analysis of human participation in digital platforms in the age of surveillance capitalism. *REAd. Revista Eletrônica de Administração (Porto Alegre)*, *26*(1), 176-209.
Wang, J., Yang, Y., Wang, T., Sherratt, R. S., & Zhang, J. (2020). Big Data Service Architecture: A Survey. *Journal of Internet Technology*, *21*(2), 393-405.
Wedel, M., & Kannan, P. (2016). Marketing analytics for data-rich environments. *Journal of Marketing*, *80*(6), 97-121.
Weinstein, A. (2020). Creating Superior Customer Value in the Now Economy. *Journal of Creating Value*, *6*(1), 20-33. https://doi.org/10.1177/2394964319898962
West, S. M. (2019). Data Capitalism: Redefining the Logics of Surveillance and Privacy. *Business & Society*, *58*(1), 20-41. https://doi.org/10.1177/0007650317718185
Wood, D. M., & Monahan, T. (2019). platform surveillance. *Surveillance & Society*, *17*(1/2), 1-6.
Yeung, K. (2018). Five fears about mass predictive personalization in an age of surveillance capitalism. *International Data Privacy Law*, *8*(3), 258-269.
Yu, M., Zhuge, J., Cao, M., Shi, Z., & Jiang, L. (2020). A Survey of Security Vulnerability Analysis, Discovery, Detection, and Mitigation on IoT Devices. *Future Internet*, *12*(2), 27.
Yu, T. R., & Song, X. (2020). Big Data and Artificial Intelligence in the Banking Industry. *World Scientific Book Chapters*, 4025-4041.
Ziemba, W. T. (2020). The COVID-19 Crash in the US Stock Market. *Available at SSRN 3632410*.
Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*(1), 75-89.
Zuboff, S. (2016). *The Secrets of Surveillance Capitalism*. Frankfurter Allgemeine Zeitung. https://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html
Zuboff, S. (2019a). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Public Affairs.
Zuboff, S. (2019b, Sep 23, 2019). *Shoshana Zuboff on 'surveillance capitalism' and how tech companies are always watching us* [Interview]. https://www.youtube.com/watch?v=QL4bz3QXWEo
Zuboff, S. (2019c). Surveillance Capitalism and the Challenge of Collective Action. *New Labor Forum*, *28*(1), 10-29. https://doi.org/10.1177/1095796018819461